

ISO 17799: Asset Management

By Gregory Yhan, CISSP, MCAD.Næ

Introduction

In a previous article, I outlined the scope and implementation guidelines for the ISO 17799 information security standard. The article also examined Security Policy, the first of eleven security clauses mentioned in the standard. The ISO 17799 defines the term asset as 'anything that has value to an organization.' In the realm of information technology, assets can range from data files to physical assets, such as removable media; however, the ISO definition allows an organization to classify items as assets from a broader spectrum. Intangibles, such as reputation of the organization, general utilities, and the skill sets of a workforce can all be classified as assets. The following article will examine the 'Asset management' security clause, including the two main security categories listed under this clause.

Responsibility for assets

'Responsibility for assets' is the first of two main security categories listed under the Asset management clause. According to the ISO, the overall objective of asset responsibility is to achieve and maintain adequate protection of assets. To achieve this objective, the 17799 standard has listed three controls. Inventory of Assets, Ownership of assets and acceptable use of assets, collectively or individually implemented will enable an organization to maintain appropriate protection of assets.

Inventory of assets

As aforementioned, Inventory of Assets is one of three controls listed under the main security category, Responsibility of assets. As the phrase implies, Inventory of Assets requires assets to be clearly identified and an inventory of 'important' assets be created for an organization. According to the implementation guidelines offered by the ISO, the importance of each asset should also be documented. The importance of an asset can be measured by its business value and security classification or label. The inventory should include all necessary information required for an organization to recover from a 'disaster.' Depending on an organization, inventories of assets will not only allow for effective protection of assets but also may be required for other business processes, such as insurance or financial reasons. The ISO 17799 also highlights that an inventory is an important prerequisite for risk management.

Ownership of assets

The second of three controls listed under the Responsibility for assets main security category is Ownership of assets. According to the ISO, all information and assets associated with 'information processing facilities' should be 'owned' by a designated part of the organization. In the 17799 standard, information processing facilities is defined as 'any information processing system, service or infrastructure, or the physical locations housing them.' The term 'owner' identifies an 'individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.' Therefore, ownership can be allocated to an application, a business process or a defined set of data. The standard further warns that the term does not mean that the person has any property rights to the asset. The designated owner of an asset should ensure that information and assets associated with processing facilities are properly classified. In addition, the owner is responsible for defining and reviewing access classifications.

Acceptable use of assets

The last of three controls listed under the Responsibility of assets security category is 'Acceptable use of assets.' This control assists in maintaining protection of assets by identifying, documenting and implementing rules for the acceptable use of information and assets. The organization is expected to establish rules for the acceptable use of information and assets. These include, but are not limited to, email and Internet usage. The key to a successful 'use of asset' policy is one that is supported by management. The goal is to make all employees and even contractors aware of the limits that exist regarding the use of their organization's information and assets.

Information classification

Information classification is the last of two main security categories listed under the Asset management security clause. Instead of achieving and maintaining adequate protection of assets, the objective of information classification is to ensure that information receives the appropriate level of protection. Information should be classified to indicate the expected degree of protection when handling the information. The ISO 17799 has listed two controls to meet this objective, Classification guidelines and Information labeling and handling.

Classification guidelines

According to this control, information should be classified in terms of its 'legal requirements, sensitivity, and criticality' to an organization. The implementation guidance (do you mean guidelines?) sheds further light on these requirements. The classification guidelines should consider the business needs for sharing or restricting information. This evaluation will lead to a clearer understanding of what information needs to be protected and the possible impact these measures will have on business rules. The responsibility of classification falls within the asset owner's domain. It is the owner's responsibility to review and update classification levels. The need for continued review stems from the fact that information ceases to be sensitive or critical after certain periods of time. The ISO warns that 'over-classification' can lead to implementing unnecessary controls leading to additional expense.

Information labeling and handling

The second control under this security category involves developing procedures for labeling and handling information according to the classification scheme adopted by an organization. These procedures should consider labeling information in its electronic and physical formats. For example, the output from certain systems classified as critical should be labeled. These labeling rules should reflect the rules set out in the classification guidelines mentioned above. Each classification level should define procedures for processing, storage, transmission, declassification and destruction of assets. As the sharing of information becomes more critical for the success of businesses, labeling and secure handling of information is key for security.

Conclusion

Managing and securing an organization's assets can be a daunting task. The ISO 17799 Asset management security clause has laid out a strong foundation from which organizations can implement appropriate controls for protecting assets. Developing an inventory of assets, defining owners of assets, establishing acceptable use policies, and classifying and labeling information are all controls that can be implemented to ensure information and assets receive appropriate protection.